



HP WOLF PRO SECURITY

DATASHEET



HP WOLF SECURITY

Uitgebreide pc-beveiliging op een eenvoudige manier.



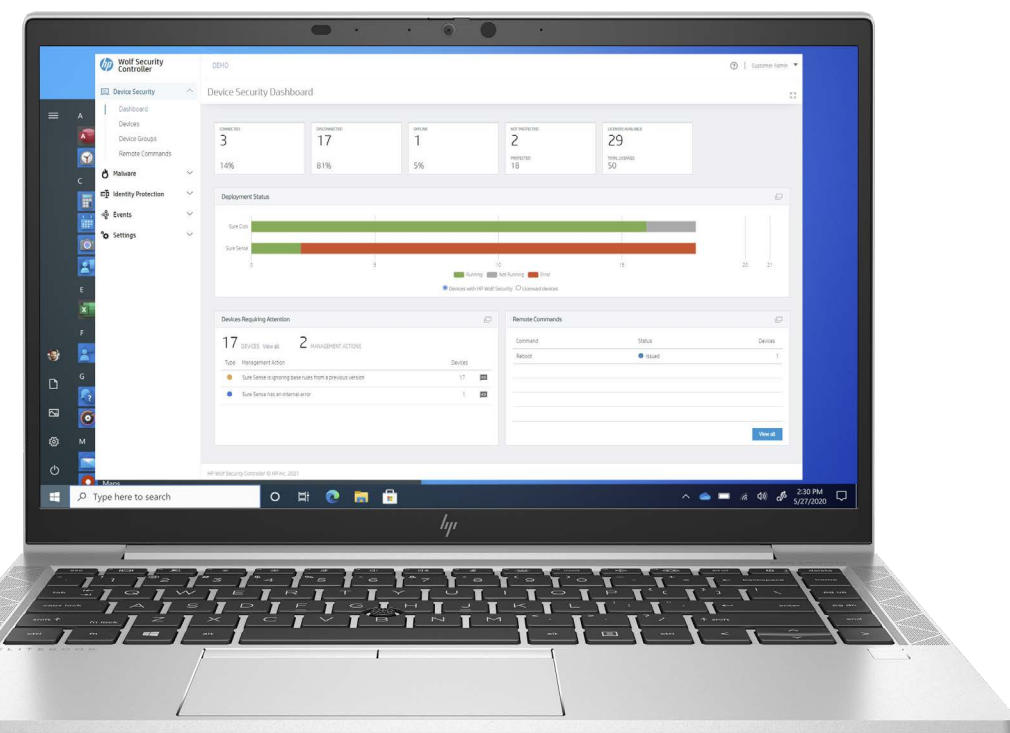
Vanwege te weinig personeel en training op het gebied van beveiliging zijn kleine tot middelgrote bedrijven kwetsbaar voor cyberaanvallen zoals phishing en ransomware. Deze aanvallen leiden tot problemen die veel geld kosten, waaronder aangetaste systemen, gestolen gegevens en langdurige uitval van apparatuur.

HP Wolf Pro Security (WPS) helpt kleine en middelgrote bedrijven deze uitdagingen te overwinnen met een eenvoudige oplossing die maximale beveiliging biedt zonder de werklast van de IT-afdeling te vergroten of de productiviteit van werknemers te onderbreken.

EENVOUDIGE BEVEILIGING DIE EENVOUDIG TE INSTALLEREN EN TE BEDIENEN IS

HP WPS is een complete oplossing voor endpointbeveiliging die is ontwikkeld met eenvoud als uitgangspunt. Hij omvat recht-toe-recht-aan beleidsbeheer, eenvoudig onderhoud en continu beheer van waarschuwingen, waardoor hij gemakkelijk geïnstalleerd en beheerd kan worden.

HP Wolf Security Controller



Een controller in de cloud, de HP Wolf Security Controller¹, biedt een centraal 'commandocentrum' voor het beheren van de beveiliging en status van alle pc's van het bedrijf, waardoor beheerders ongeacht waar ze zijn het beveiligingsbeleid kunnen aanpassen en inzichten over dreigingen kunnen beoordelen.

Vooraf geconfigureerd "out-of-the-box"-beleid zorgt er voor dat de oplossing in de meeste omgevingen snel is te installeren, eenvoudig is te begrijpen en weinig continue afstemming vereist.

Continue veiligheidswaarschuwingen maken eindgebruikers attent op kwaadwillende activiteiten. Ze worden alleen verstuurd wanneer de aandacht van de gebruiker is vereist en maken het vaststellen van verdachte activiteit op de pc eenvoudiger.

PERSONEEL BESCHERMEN ZONDER HEN VAN HUN WERK AF TE HOUDEN

Werknemers zijn geen beveiligingsexperts en het is niet reëel om van hen te verwachten dat ze altijd alert zijn op het herkennen van socialengineeringaanvallen. Beveiligingsmaatregelen die werknemers belemmeren in hun werkzaamheden, voldoen niet in bedrijven die van hun werknemers verwachten dat ze veilig werken en productief zijn.

HP WPS levert uitgebreide endpointbeveiliging die pc-gebruikers beschermt en zorgt daarmee voor een positieve gebruikerservaring van werknemers. Dit leidt tot een hogere productiviteit terwijl tegelijkertijd hun gegevens en wachtwoorden en de systemen van het bedrijf beschermd zijn.

Werknemers hoeven zich geen zorgen te maken met een beveiligingsoplossing die achter de schermen werkt en geen belemmering vormt voor hun dagelijkse werkzaamheden.

Werknemers hoeven niet langer te fungeren als “beveiligingssensoren” en kunnen vol vertrouwen bijlagen en links openen, in de wetenschap dat HP WPS gebruikmaakt van insluitingstechnologie om bedreigingen te isoleren.

Werknemers kunnen overal veilig werken dankzij insluitingstechnologie die ook werkt als de pc niet is verbonden met internet, waardoor de bescherming altijd actief is.

BEPROEFDE BESCHERMING WAAR JE VAN OP AAN KUNT

HP WPS gebruikt beveiligingstechnologie waarvan is bewezen dat de klanten van HP hiermee goed worden beschermd. Op pc's met HP Wolf Security-technologie zijn meer dan 10 miljard e-mailbijlagen, webpagina's en downloads geopend zonder meldingen van een aangetast apparaat.

HP WPS omvat drie functies, die allemaal worden beheerd via de Wolf Security Controller.

Met **hardwarematige insluiting van bedreigingen**² worden malware-aanvallen via social engineering of andere methoden geïsoleerd en ingesloten, waardoor wordt voorkomen dat de pc, of iets anders op het netwerk, besmet raakt.

Met **bescherming van inloggegevens tegen phishing** wordt de diefstal van inloggegevens voorkomen door het blokkeren van phishingaanvallen waarbij wordt geprobeerd gebruikers zover te krijgen dat ze hun wachtwoord invoeren op een nepwebsite.

Met **antivirus van de volgende generatie** worden opkomende bedreigingen gedetecteerd door AI met deep learning, als aanvulling op het stoppen van bekende malware.



DE VOORDELEN VAN EEN EENVOUDIGE BEVEILIGINGSOPLOSSING DIE IS ONTWERPEN VOOR GEBRUIKSVRIENDELIJKHEID EN WERKNEMERSPRODUCTIVITEIT

HP Wolf Pro Security is het meest geschikt voor bedrijven die zich bij hun investeringen in IT-ondersteuning en -personeel richten op maximale mogelijkheden en productiviteit voor gebruikers. Door de traditionele antivirusprogramma's te vervangen door HP WPS, is het bedrijf beter beschermd en is er minder noodzaak om beveiligingsexperts in dienst te hebben. Hiermee komen middelen vrij die ingezet kunnen worden voor taken met een hogere waarde.

- **Geringe mate van inspanning** bij de installatie en het lopende onderhoud is gecentraliseerd en vereenvoudigd
- **Lager risico** met een aanpak voor endpointbeveiliging waarbij de preventieve bescherming voorop staat, waaronder realtime bescherming met AI en zero-trust, hardwarematige isolatie
- **Vereenvoudigde installatie** zonder beheerinfrastructuur op locatie

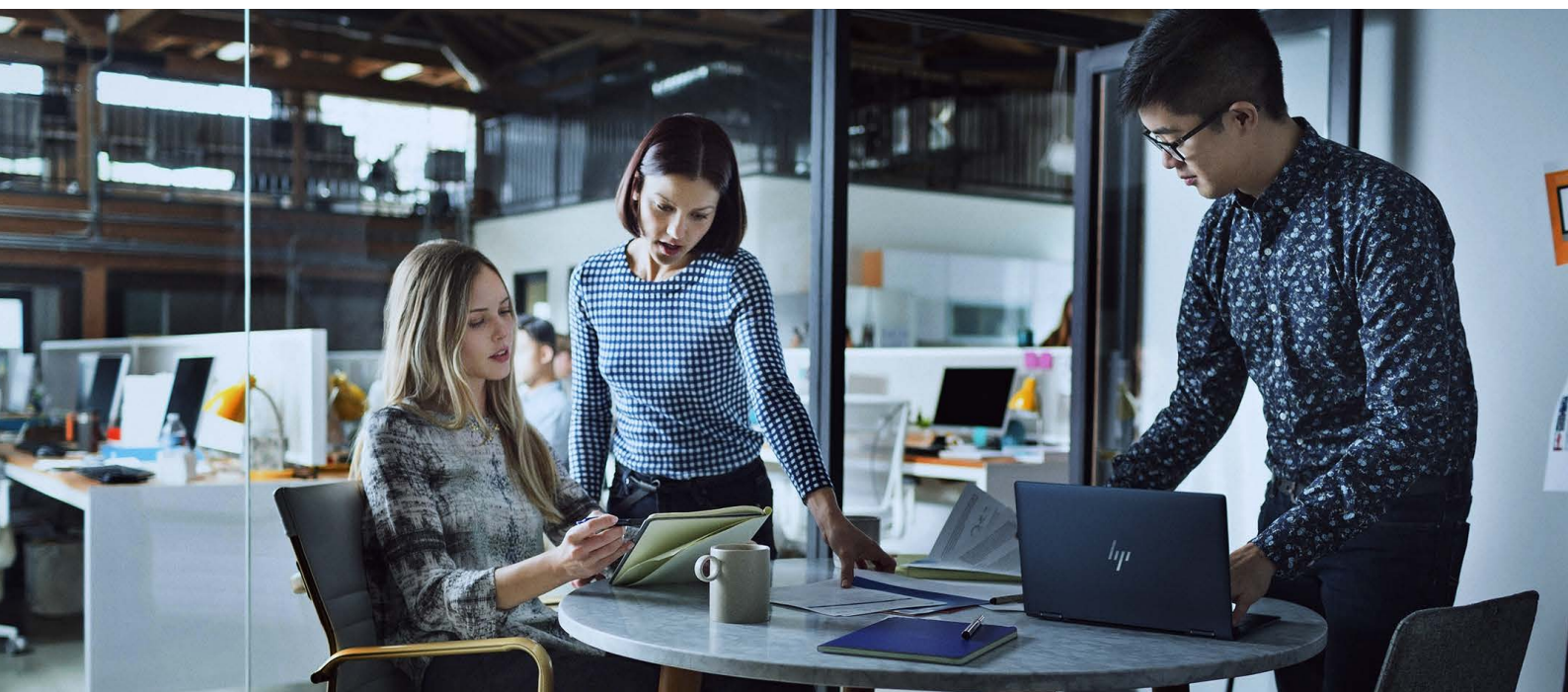
FLEXIBELE OPTIES VOOR ELKE SITUATIE

HP Wolf Pro Security is verkrijgbaar in verschillende gebruiksopties, voor een consistente beveiligingsoplossing die aansluit bij je behoeften. Je kunt het vooraf geïnstalleerd kopen op pc's met de HP Wolf Pro Security Edition³ of als losse software (licentie voor de looptijd)⁴. Het is ook leverbaar voor pc's van andere merken, waardoor je meer flexibiliteit hebt om beveiliging van bedrijfsniveau te installeren op het apparaat van je keuze.

HP WOLF PRO SECURITY SYSTEEMVEREISTEN EN ONDERDELEN

Wolf Security Controller	Beschikbaar voor alle klanten met ten minste 25 pc's.
Onderdelen van de beveiligingssoftware	HP Wolf Pro Security-client voor Windows en HP Wolf Security cloud controller (cloud)
Ondersteunde besturingssystemen	Windows 11 64-bits; Windows 10 Pro 64-bits; Windows 10 Enterprise; Windows 10 Enterprise LTSC (alleen 64-bits)
Vereist geheugen/schijfruimte	Minimaal 8 GB systeemgeheugen (16 GB aanbevolen) / 10-20 GB vrije schijfruimte
Ondersteunde talen (endpoint)	Engels, Nederlands, Frans, Duits, Italiaans, Japans, Portugees (Brazilië), Spaans, Zweeds
Ondersteunde talen (controller)	Engels
Netwerkvereisten	Er is een internetverbinding vereist voor communicatie tussen het beheerde apparaat en de cloudbeheerservice voor dreigingsanalyse. De bescherming blijft echter ook offline normaal functioneren, er is geen netwerkverbinding vereist.
Vereisten voor activering	Om de oplossing te gebruiken, moet deze na aankoop worden geactiveerd aan de hand van de via e-mail ontvangen instructies van HP. Tijdens het activeringsproces moet je informatie opgeven die noodzakelijk is om het account- en veiligheidsbeleid te configureren.
Servicevoorwaarden	
voor HP Wolf Pro Security Edition	HP Wolf Pro Security Edition wordt vooraf geïnstalleerd geleverd op bepaalde SKU's en is inclusief een betaalde licentie voor 1 of 3 jaar, afhankelijk van het aangeschafte HP product. De HP Wolf Pro Security Edition-software valt onder de licentievoorwaarden van de HP Wolf Security Software - End-User license Agreement (EULA) die beschikbaar is op: https://support.hp.com/us-en/document/ish_3875769-3873014-16 waarbij die EULA met het volgende is aangepast: "7. Looptijd. Tenzij anderszins op een eerder tijdstip beëindigd conform de voorwaarden van deze EULA, wordt de licentie voor de HP Wolf Pro Security Edition van kracht bij activering en blijft gedurende een termijn van twaalf (12) maanden of zesendertig (36) maanden ("Initiële looptijd") geldig. Aan het einde van de Initiële looptijd kun je (a) een verlenging van je licentie voor de HP Wolf Pro Security Edition aanschaffen via HP.com, HP Sales of een HP Channel Partner, of (b) een beperkte versie van de technologie voor dreigingsisolatie, malwarepreventie en bescherming van inloggegevens blijven gebruiken zonder extra kosten en zonder toekomstige software-updates of HP ondersteuning."
voor HP Wolf Pro Security (licenties met looptijd)	HP Wolf Pro Security is verkrijgbaar bij geautoriseerde HP channel partners met een licentie voor één of drie jaar. Na afloop van de initiële looptijd kun je bij een HP Channel Partner een verlenging van de licentie voor HP Wolf Pro Security kopen. Kijk voor de volledige servicevoorwaarden op https://www.hpwolf.com/terms-and-conditions/ .

Meer informatie over [HP Wolf Pro Security](#).



DISCLAIMERS

¹ Voor de HP Wolf Pro Security Controller zijn minimaal 25 apparaten vereist.

² Voor dreigingsisolatie worden de volgende browsers voor Microsoft Windows ondersteund: Microsoft Edge, Google Chrome, Mozilla Firefox en Chromium. Tot de ondersteunde bijlagen behoren onder meer Microsoft Office (Word, Excel, PowerPoint) en pdf-bestanden, mits Microsoft Office of Adobe Acrobat is geïnstalleerd.

³ HP Wolf Pro Security Edition wordt vooraf geïnstalleerd geleverd op bepaalde SKU's en is inclusief een betaalde licentie voor 1 of 3 jaar, afhankelijk van het aangeschafte HP product. De HP Wolf Pro Security Edition-software valt onder de licentievoorwaarden van de HP Wolf Security Software – End-User license Agreement (EULA) die beschikbaar is op: https://support.hp.com/us-en/document/ish_3875769-3873014-16 waarbij die EULA met het volgende is aangepast: "7. Looptijd. Tenzij anderszins op een eerder tijdstip beëindigd conform de voorwaarden van deze EULA, wordt de licentie voor de HP Wolf Pro Security Edition van kracht bij activering en blijft gedurende een termijn van twaalf (12) maanden of zesendertig (36) maanden ("Initiële looptijd") geldig. Aan het einde van de Initiële looptijd kun je (a) een verlenging van je licentie voor de HP Wolf Pro Security Edition aanschaffen via HP.com, HP Sales of een HP Channel Partner, of (b) een beperkte versie van de technologie voor dreigingsisolatie, malwarepreventie en bescherming van inloggegevens blijven gebruiken zonder extra kosten en zonder toekomstige software-updates of HP ondersteuning."

⁴ HP Wolf Pro Security is verkrijgbaar bij geautoriseerde HP channel partners met een licentie voor één of drie jaar. Na afloop van de initiële looptijd kun je bij een HP Channel Partner een verlenging van de licentie voor HP Wolf Pro Security kopen. Kijk voor de volledige servicevoorwaarden op <https://www.hpwolf.com/terms-and-conditions/>.



HP WOLF SECURITY

© Copyright 2022 HP Development Company, L.P. De informatie in dit document kan zonder voorafgaande kennisgeving worden gewijzigd. De van toepassing zijnde garanties voor HP producten en diensten zijn vastgelegd in de uitdrukkelijke garantiebepalingen die bij dergelijke producten en diensten op fysieke en/of elektronische wijze worden meegeleverd of gepubliceerd op website(s) van HP. Niets in dit document mag als een aanvullende garantie worden opgevat. HP is niet aansprakelijk voor technische en/of redactionele fouten c.q. weglatingen in dit document.

Microsoft en Windows zijn geregistreerde handelsmerken of handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen. Intel en Core zijn handelsmerken van Intel Corporation of zijn dochterondernemingen in de VS en/of andere landen.

4AA8-1150NLE, januari 2022